

## Chapter 2

# Resilience Engineering: The Birth of a Notion

Christopher P. Nemeth

Sidney Dekker's chapter in *Resilience Engineering: Concepts and Precepts* (Dekker, 2006) strove to capture the ideas that emerged during the first resilience engineering symposium held in Söderköping, Sweden in October, 2004. The notion of resilience as an aspect of systems appeared to resonate among the fourteen senior researchers who participated. Their discussion centered on the need to:

- Get smarter at reporting the next [adverse] event, helping organizations to better manage the processes by which they decide to control risk
- Detect drift into failure before breakdown occurs. Large system accidents have revealed that what is considered to be normal is highly negotiable. There is no operational model of drift.
- Chart the momentary distance between operations as they are, versus as they are imagined, to lessen the gap between operations and management that leads to brittleness.
- Constantly test whether ideas about risk still match reality. Keeping discussions of risk alive even when everything looks safe can serve as a broader indicator of resilience than tracking the number of accidents that have occurred.

My contribution is to extract the themes that flowed through the three days of presentation and discussion at the second RE Symposium in November, 2006 at Juan-Les-Pin, France. Differences between those who participated in the first and second symposia affected the content and character of discussion. In the first symposium, fourteen senior researchers (most of whom knew each other) wrestled with the notion

of resilience as a perspective on system safety. In the second symposium, a much larger audience of eighty participants reflected the rapidly growing interest in the topic. The more diverse composition of this group was a consequence of the organizers' efforts to invite those who are studying as well as practicing in the field to participate in shaping the discussions.

Among the lively exchanges, four themes seemed to recur with some regularity. The text that expands on each theme is intended to show the variety of insights that were exchanged.

## **Understand the Nature of Systems and Environments**

As a newly evolving concept, discussions explored the nature of resilience, how systems are developed to operate in an expected environment, and how they evolve and respond to the environments in which they operate.

Resilience seems to be closely linked with some sort of insight into the (narrowly defined) system, the (broadly defined) environment in which it exists, and their interactions.

Traditionally, "systems" have been defined according to what can be managed, leaving ill-behaved elements outside of their boundaries. Most of the resilience of systems involves the interaction between engineered components and their environment. Much of what we see in inquiries about resilience is actually inquiry into where the boundary between the system and environment should be.

Resilience involves anticipation. This includes the consideration of how and why a particular risk assessment may be limited, having the resources and abilities to anticipate and remove challenges, knowing the state of defenses now and where they may be in the future, and knowing what challenges may surprise. Taking a prospective view assumes that challenges to system performance will occur, and actively seeks out the range and details of these threats.

Operators who have a deep understanding of an application area are an important source of resilience. This is expertise in action. Deeper understanding allows at least two sources of resilience. One is to know sooner when "things are going wrong" by picking up faint signals of impending dysfunction. The other is to have better knowledge resources that are available in order to develop adaptive resources "on

the fly.” It follows that the lack of such understanding diminishes resilience. It also follows that resulting choices that lack an understanding of how to create, configure, and operate a system lead to less resilient (more brittle) systems. Resilience can be seen in action, and is made visible through the way that safety and risk information are used. Resilience is an active process that implicitly draws on the way that an organization or society can organize itself. It is more than just a set of resources because it involves adaptation to varying demands and threats. Adaptation and restructuring make it possible for an organization to meet varying, even unanticipated, demands.

Resilience requires rules to be ignored under some conditions, but when? Dilemmas are embedded in the ways that systems operate. Procedures and protocols direct activity, but why follow procedures when judgment suggests a departure is prudent? On the other hand, what evidence do we have that the individual judgment will be correct when stepping outside of what has already proven to be reliable? Rules are intended to control performance variability. Enchantment with procedures, though, can lead to excessive reliance on rules and insufficient reliance on training. The adoption of automation in a work setting can increase this tendency. Engineered systems are designed to operate within, but not outside, certain conditions. Automation has been touted as a means to improve system flexibility. How can automation improve the fit between environment and engineered system when it is inherently part of that system?

## **Differentiate between Traditional and Evolving System Models**

Traditional risk assessment typically deals with a small number of possible scenarios that are considered as a moment in time. These are treated simplistically in ways that do not adequately reflect the complexities of human behavior or of large systems. Risk assessment tries to anticipate both the type and scale of future failures, but there are constraints in our ability to anticipate complex events both from our limited ways to imagine the future and from the limits of risk assessment technology. By contrast, resilience shifts attention to a prospective view by anticipating what future events may challenge system performance. More importantly, resilience is about having the

generic ability to cope with unforeseen challenges, and having adaptable reserves and flexibility to accommodate those challenges.

Few organizations have set up measurement systems to monitor performance change. The traditional notion of reliability amounts to the addition of structure in a stable environment. By contrast, resilience invests flexibility and the ability to find and use available resources in a system in order to meet the changes that are inherent in a dynamic world.

Resilience might be considered from the viewpoint of a system's output in response to demand, through time. How the system responds can determine its ability to either meet demand, make up for a lag in output when it falls short, or restructure in order to meet a new quality or level of demand that was not previously anticipated. Making changes to systems in anticipation of needs in order to meet future demands is the engineering of resilience.

Conferees discussed approaches to engage issues that are related to resilience including simulation, top-down conceptual models, and field research. In field work, the observation of work can reveal *work as done*, versus *work as imagined*. For example, the study of a nuclear power plant control room in Brazil demonstrated how granular level observation made it possible to appreciate informal initiatives that workers take to make resilience work.

Unexampled events are rare occurrences in the flow of daily work that are so unlikely that system developers do not consider the need to defend against them. In a well-tested system there is no drift into danger. Accidents are instead part of the distribution of events. Even though they are rare, if there is a failure the probability is it's a bad one. Dictionaries define resilience as elasticity, or a rebounding. To measure something, we must know its essential properties. Resilience of materials must be measured by experiment in order to find how much a material returns to its original shape. The same can be said for systems. The act of measurement is the key for engineers to begin to understand the nature of an unexampled event, and the probability part of Probabilistic Risk Assessment (PRA). In PRA, the act of trying to assign values has its own value. This suggests a second culture to explore and evaluate the possible, not the probable.

The traits of resilience include experience, intuition, improvisation, expecting the unexpected, examining preconceptions, thinking outside the box, and taking advantage of fortuitous events. Each trait is complementary, and each has the character of a double-edged sword.

## **Explore the Breadth and Degree of Resilience in Various Settings**

Environments and the systems that are created to operate in them vary significantly. Unusual or changing demands impose requirements on system performance across a number of applications that can threaten their survival.

*Healthcare* – A system can be pushed beyond its ability to perform and restore itself. The account of a 79-bed hospital emergency department in “free fall” for seven hours demonstrated how clinicians created additional means to accept and manage patients (Wears, Perry & McFauls, 2006). Patient convenience and clinician comfort were traded-off for the ability to accept a level of patient population that taxed the staff well beyond its intended ability to cope. The attending physician’s decision to give up control and redistribute it to residents allowed the system to continue operating, and surviving, while performing at a lower level.

Extreme environments involve exceptional risk and pose the greatest need for resilience.

*Commercial fishing* – In the United Kingdom and the U.S., one in eight commercial fishing workers is injured annually. Regulation has been used to manage other similar sectors such as construction and transportation, but the commercial fishing industry is hard to regulate and manage. This is because fleets must follow the fish in order to generate revenue. Their willingness to accept risk in order to assure revenue is one of many reasons that makes fishing resistant to change.

*Chemical and power plants* – Commercial firms make technological and organizational changes to increase profit while at the same time maintaining a perceived level of safety. Even though adverse events are not occurring, how does a firm maintain awareness to understand issues related to safety while simultaneously benefiting operations? In short, “what is happening when nothing is happening?”

Resilience is based on system ecology and promotes system survival. Safety is often a topic of resilience discussions, but there is more to resilience than safety. Is a resilient system a safe system? What is the relationship between resilience and safety? Are systems evaluated differently in different domains? Is resilience the absence of accidents or incidents, or the ability to learn from incidents? How do long periods of little perceived change in demand invite cuts to system resources in order to conserve costs or increase profits? Can resilience management better promote survival in terms of both commercial and safety pressures?

## Develop Ways to Capture and Convey Insights into Resilience

Systems' level research continues to confront issues in methods. Following a system-level approach runs the risk of imposing a model on reality, rather than eliciting data to determine whether the model reflects properties that are consistent with it.

Lack of familiarity with an application area can cause the researcher to miss the deeper aspects that have formed it. Those who make brief visits to operational facilities can get the impression that they understand what occurs there. However, they miss the substantive and often intractable influences workers have to negotiate every day that are not apparent to one who visits occasionally or for a short time.

Methods to communicate about resilience also need research attention. Representations of resilience are still in the early stages. Richer ways to depict the actual nature of systems promise to close the gap between operations and management. For example, managers of Brazilian nuclear power plant operations were not aware of actual operations in plant control centers until a thorough description of observational studies revealed *work as done*.

## Conclusions

A successful research symposium doesn't provide answers, but rather broadens and deepens the quality of inquiry and learning. Participants posed a number of questions that only further research can address. What continues to push systems toward becoming more brittle? What

limits exist, or should exist, over system design in research and development or in operations? Expanding the base of participants expands the scope of inquiry, yet softens the edge of discussions. The cordiality of those who had recently met can, and should, mature into a candid clash of thoughts to reach new levels of insight. The test of how well the notion of resilience grows will be how it matures into future research and publication.

## **Acknowledgement**

Dr. Nemeth thanks John Wreathall and Richard Cook, MD for providing valuable comments on in-progress drafts of this paper. Sandra Nunnally transcribed notes of the presentations and discussion, and Kyla Steele generously provided her own extensive notes of the sessions. Dr. Nemeth's participation in the symposium was made possible by support from the U.S. Food and Drug Administration and the Department of Anesthesia and Critical Care of The University of Chicago.

# Resilience Engineering Perspectives

Volume 1: Remaining Sensitive to the Possibility  
of Failure

*Edited by*

ERIK HOLLNAGEL

*École des Mines de Paris, Centre for Research on Risk and Crises, France*

CHRISTOPHER P. NEMETH

*The University of Chicago, USA*

SIDNEY DEKKER

*Lund University, Sweden*

ASHGATE